the standard in safety

FTA / FMEA Safety Analysis Model for Lithium-ion Batteries

NASA Aerospace Battery Workshop

Thomas Lanzisero, Anura Fernando
Underwriters Laboratories, Inc.
Corporate Research, Predictive Modeling & Risk Analysis

November 19, 2009

V1.4

Outline

- Scope
- Safety Strategy: Objective, Approach, Challenges
- FTA (Fault Tree Analysis) Safety Model
- FMEA (Failure Modes and Effects Analysis) Safety Model
- ➢ **INTEGRATED FTA / FMEA SAFETY MODEL**
- Conclusions
- Next Steps

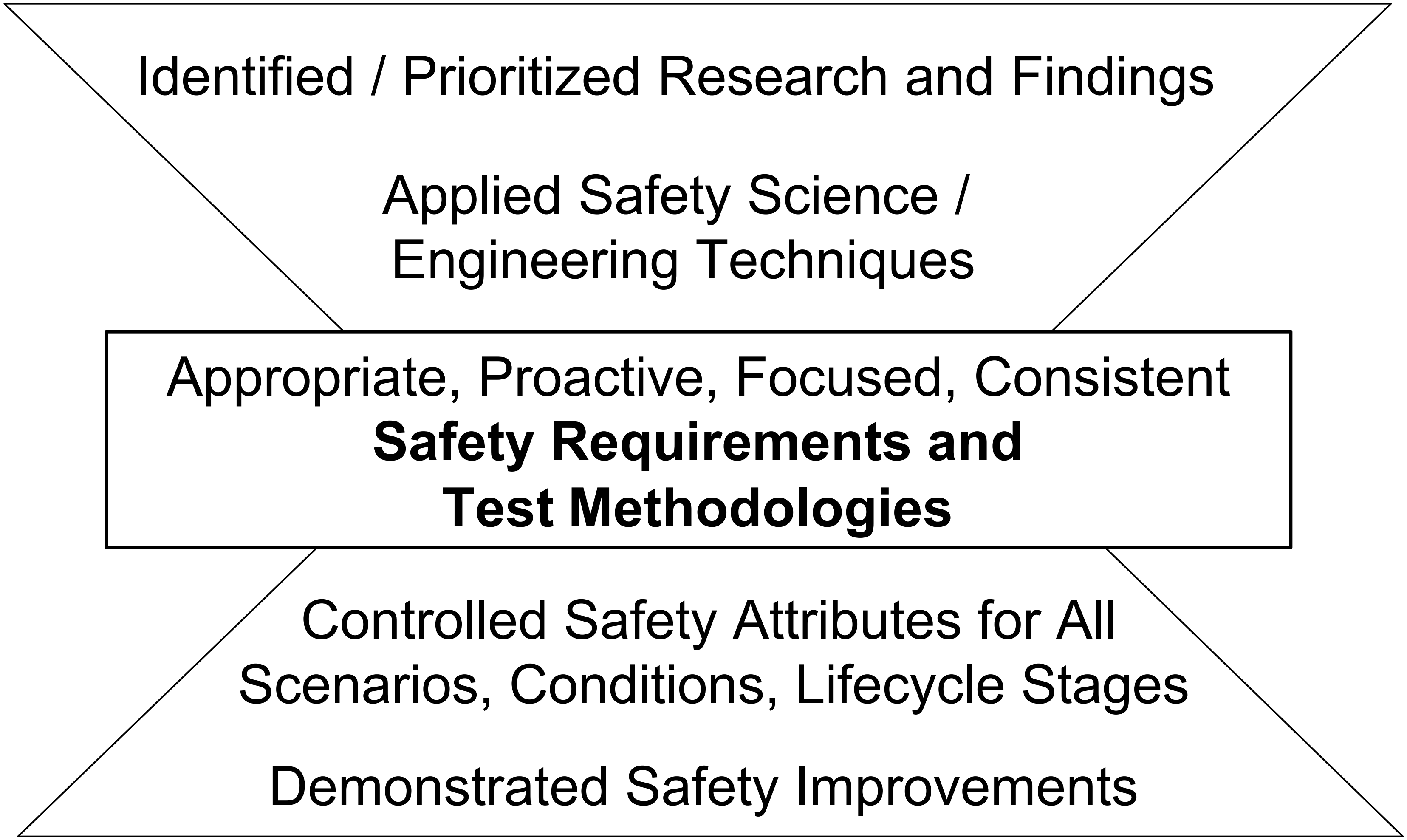
The robustness of system reliability review and root cause analysis relies on the use of a systematic approach and appropriate methods and tools, particularly important when the focus is on safety.

Scope

- Initial – COTS 18650: Single, lithium ion, cylindrical cells, secondary (rechargeable), nominal 3.4 - 4.0 V, 1200 - 2800 mAh, $LiCoO_2$ Lithium Cobalt Oxide and Lithium Ion Polymer (for ITE / CE), $LiMn_2O_4$ Lithium Manganese Oxide (for power tools)

- Future – Initial scope to be adapted / expanded as needed to cover other chemistries, designs, sizes, packs, modules, applications, etc.)

Safety Strategy



Identified / Prioritized Research and Findings

Applied Safety Science / Engineering Techniques

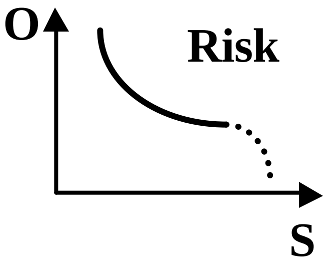
Appropriate, Proactive, Focused, Consistent **Safety Requirements and Test Methodologies**

Controlled Safety Attributes for All Scenarios, Conditions, Lifecycle Stages

Demonstrated Safety Improvements

Systematic Objective / Approach

- Define, Analyze, Validate, Control, Document
  - Safety, Risk, Harm, Hazard
- Risk Management – iterative / continual
  - Analyze, Estimate, Evaluate, Reduce, Control



- Systems Engineering
  - Subsystems, Components, Envir. – interfaces / interactions
  - Lifecycle: Design, Production, Assembly, Storage, Transport, Installation, Use, Service, Disposal, etc.
- Disciplined Analysis: harm, hazard, fault / failure
  - Means of Harm – root causes, conditions, events, mechanisms
  - Means of Protection – focused on specific means of harm

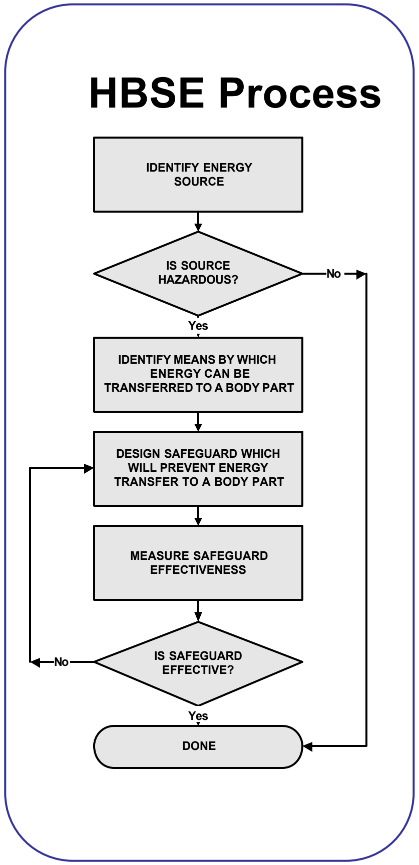
Hazard-Based Safety Engineering

Haz?

How?

Prot how?

How well?



HBSE Process

IDENTIFY ENERGY SOURCE

IS SOURCE HAZARDOUS?

No

Yes

IDENTIFY MEANS BY WHICH ENERGY CAN BE TRANSFERRED TO A BODY PART

DESIGN SAFEGUARD WHICH WILL PREVENT ENERGY TRANSFER TO A BODY PART

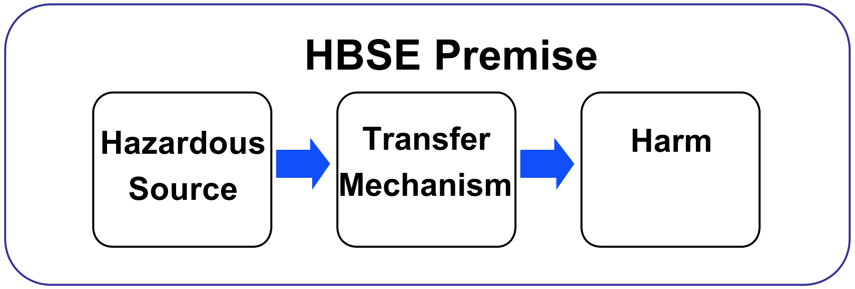
MEASURE SAFEGUARD EFFECTIVENESS

IS SAFEGUARD EFFECTIVE?

No

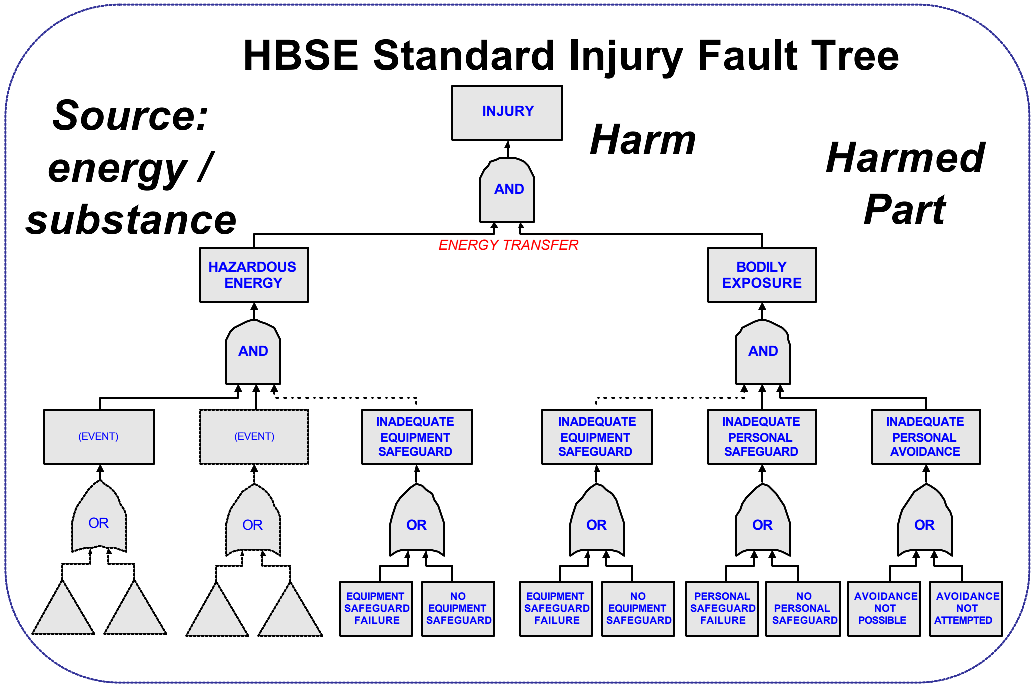
Yes

DONE



HBSE Premise

Hazardous Source → Transfer Mechanism → Harm



HBSE Standard Injury Fault Tree

Source: energy / substance

Harm

Harmed Part

INJURY

AND

ENERGY TRANSFER

HAZARDOUS ENERGY

BODILY EXPOSURE

AND

AND

(EVENT)

(EVENT)

INADEQUATE EQUIPMENT SAFEGUARD

INADEQUATE EQUIPMENT SAFEGUARD

INADEQUATE PERSONAL SAFEGUARD

INADEQUATE PERSONAL AVOIDANCE

OR

OR

OR

OR

OR

OR

EQUIPMENT SAFEGUARD FAILURE

NO EQUIPMENT SAFEGUARD

EQUIPMENT SAFEGUARD FAILURE

NO EQUIPMENT SAFEGUARD

PERSONAL SAFEGUARD FAILURE

NO PERSONAL SAFEGUARD

AVOIDANCE NOT POSSIBLE

AVOIDANCE NOT ATTEMPTED

E.g., LIB chemical potential energy converted to hazardous electrochemical and thermal energy, and sufficient amount transferred (rate, duration, concentration) to ignite combustible materials

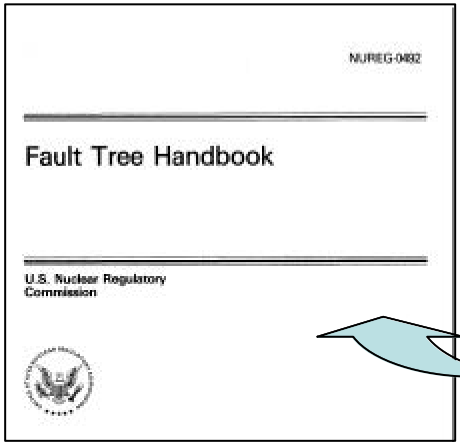
Challenges

- Integration: Techniques, Tools, Team
- Analysis → Developed Requirements:
  - Scope Management (creep, dive)
  - R&R Test Methodologies (conditions, criteria)

    Reproducible & Repeatable (consistent)

    Representative & Robust (worst-case)
  - Safety-Critical Features / Attributes:
    - Suitably identified, validated, controlled
    - Retained in all conditions, entire lifecycle
    - Effective, durable, reliable

FTA Safety Model - Overview

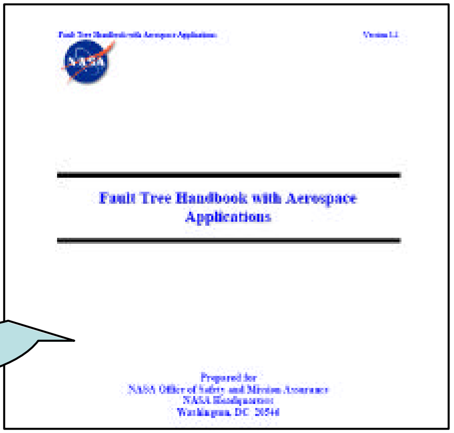


NUREG-0492

Fault Tree Handbook

U.S. Nuclear Regulatory Commission

Based on standard format / guidelines e.g., Fault Tree Handbook US NRC, NASA, etc.

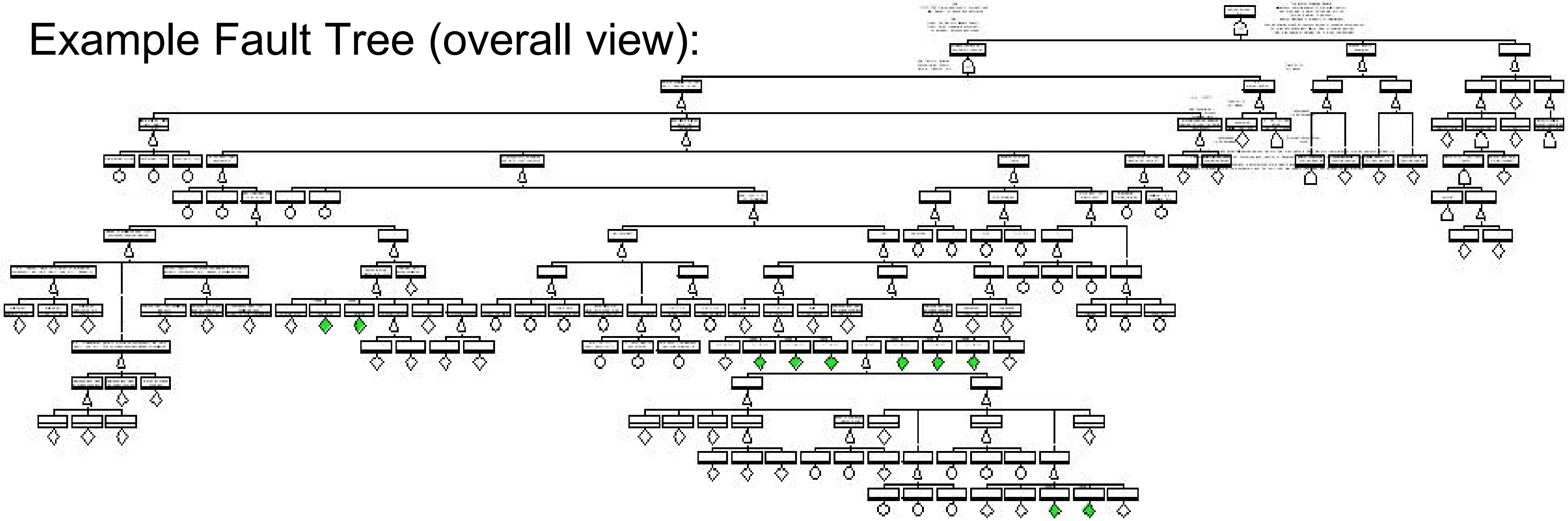


Fault Tree Handbook with Aerospace Applications Version 1.1

Fault Tree Handbook with Aerospace Applications

Prepared for
NASA Office of Safety and Mission Assurance
NASA Headquarters
Washington, DC 20546

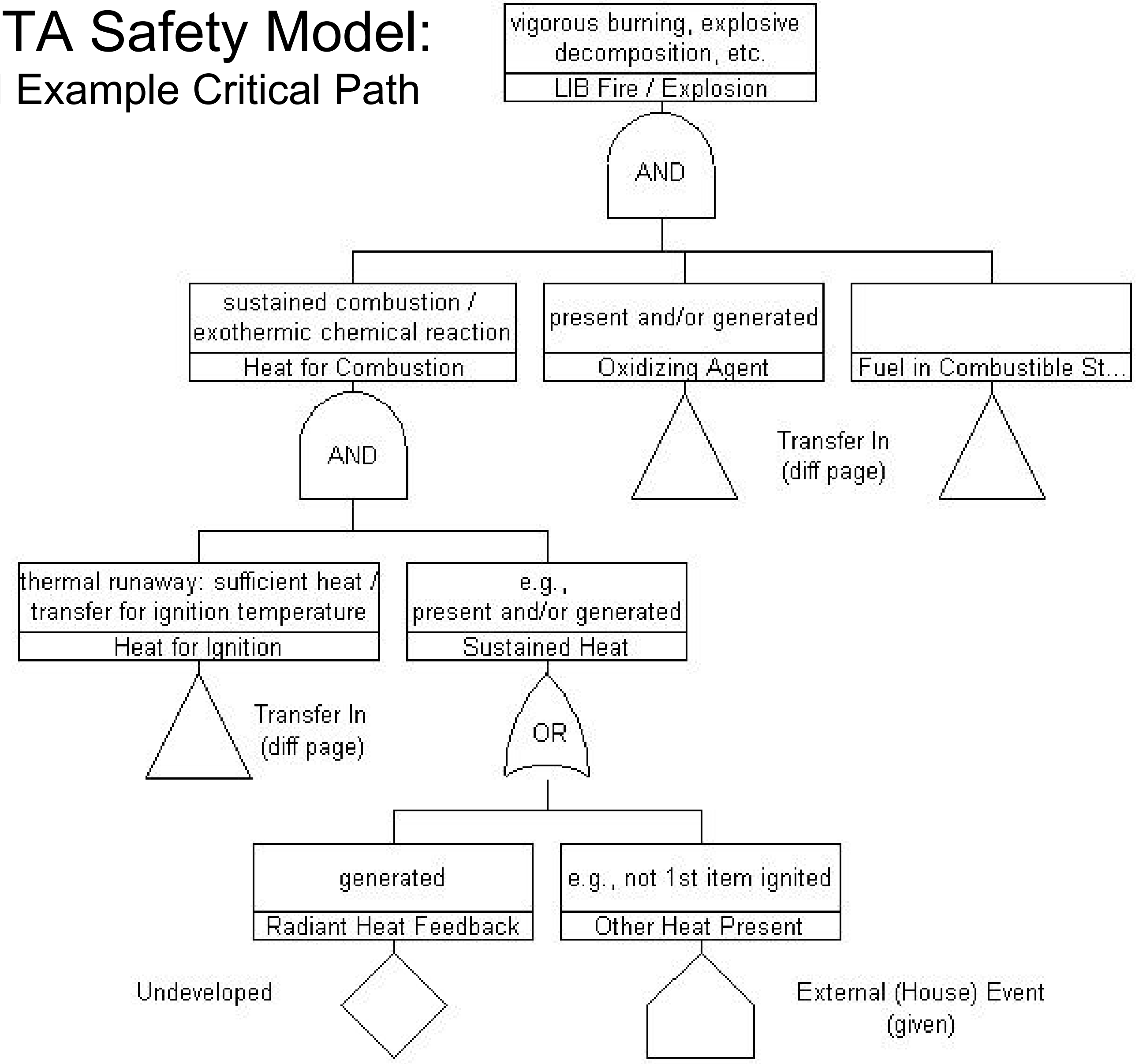
Example Fault Tree (overall view):

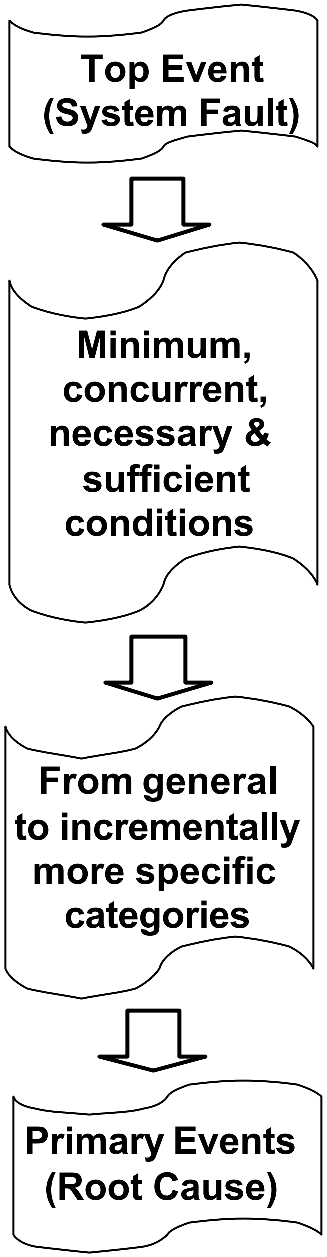


the standard in safety

LIB FTA Safety Model:

Limited Example Critical Path


vigorous burning, explosive decomposition, etc.
LIB Fire / Explosion
AND
sustained combustion / exothermic chemical reaction
Heat for Combustion
present and/or generated
Oxidizing Agent
Fuel in Combustible St...
AND
Transfer In (diff page)
thermal runaway: sufficient heat / transfer for ignition temperature
Heat for Ignition
e.g., present and/or generated
Sustained Heat
Transfer In (diff page)
OR
generated
Radiant Heat Feedback
e.g., not 1st item ignited
Other Heat Present
Undeveloped
External (House) Event (given)

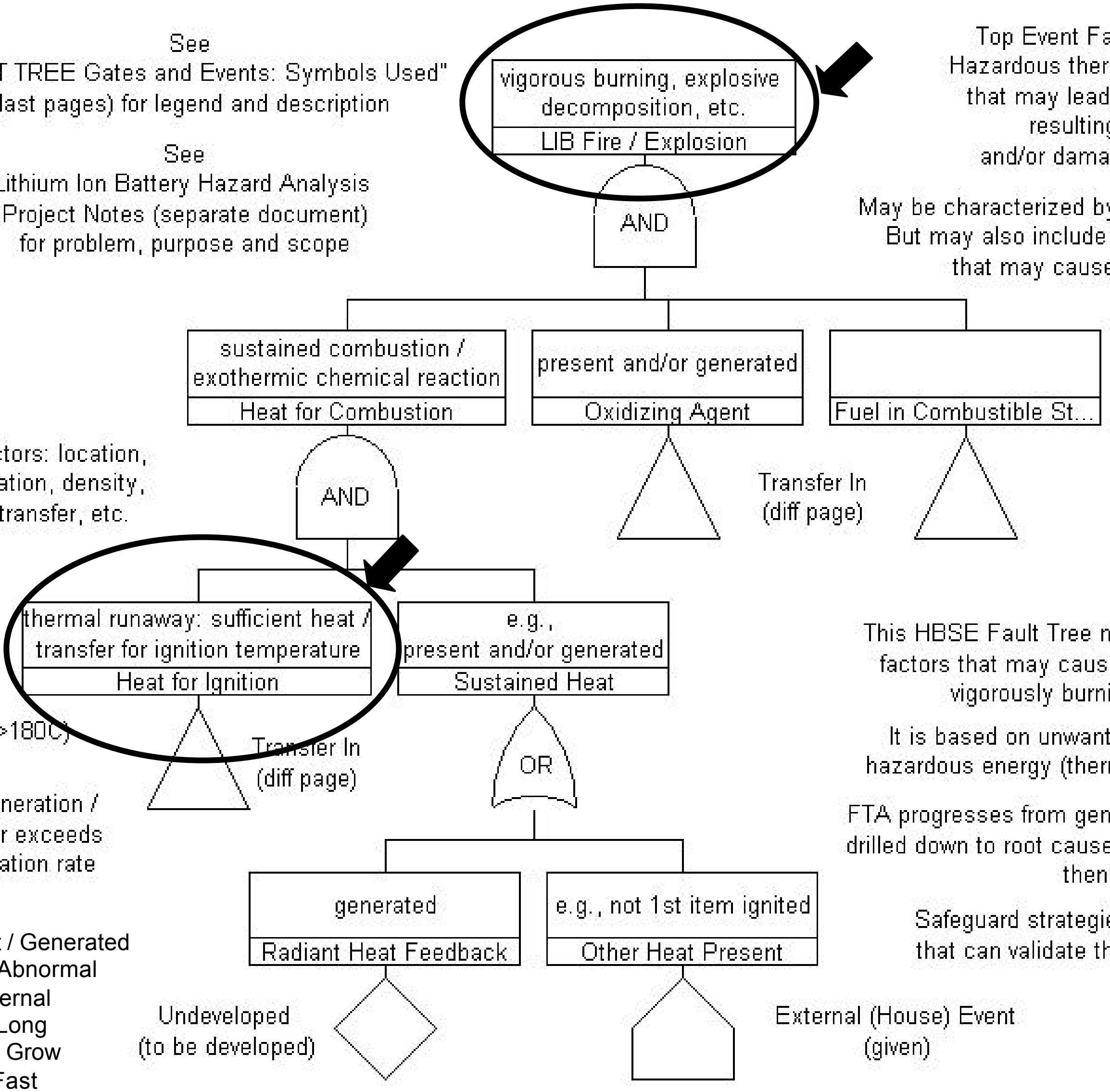

Top Event (System Fault)
Minimum, concurrent, necessary & sufficient conditions
From general to incrementally more specific categories
Primary Events (Root Cause)

the standard in safety

Need descriptions, assumptions, limitations, etc. – but let's focus on path now…

See
"FAULT TREE Gates and Events: Symbols Used"
(last pages) for legend and description

See
Lithium Ion Battery Hazard Analysis
Project Notes (separate document)
for problem, purpose and scope



vigorous burning, explosive decomposition, etc.
LIB Fire / Explosion

AND

sustained combustion / exothermic chemical reaction
Heat for Combustion

present and/or generated
Oxidizing Agent

Fuel in Combustible St...

AND

thermal runaway: sufficient heat / transfer for ignition temperature
Heat for Ignition

e.g., present and/or generated
Sustained Heat

Transfer In
(diff page)

Transfer In
(diff page)

OR

generated
Radiant Heat Feedback

e.g., not 1st item ignited
Other Heat Present

Undeveloped
(to be developed)

External (House) Event
(given)

Heat Factors: location, concentration, density, rate of transfer, etc.

(e.g., >180C)

Heat generation / transfer exceeds dissipation rate

Factors:
- Present / Generated
- Norm / Abnormal
- Int / External
- Short / Long
- Decay / Grow
- Slow / Fast
- Dissipate / Concentrate…

Top Event Fault - Fire / explosion hazard:
Hazardous thermal energy or material transfer
that may lead to harm outside battery cell,
resulting in injuries to persons,
and/or damage to property or operations.

May be characterized by vigorous burning or explosive decomposition
But may also include any flame, spark, heat or heated particles
that may cause or spread fire to other combustibles

Top Event Fault is focused on principal fire / explosion hazard, not other chemical or toxicological hazards such as from electrolyte leakage or venting, or other effects of continued combustion such as smoke opacity, toxicity or corrosivity

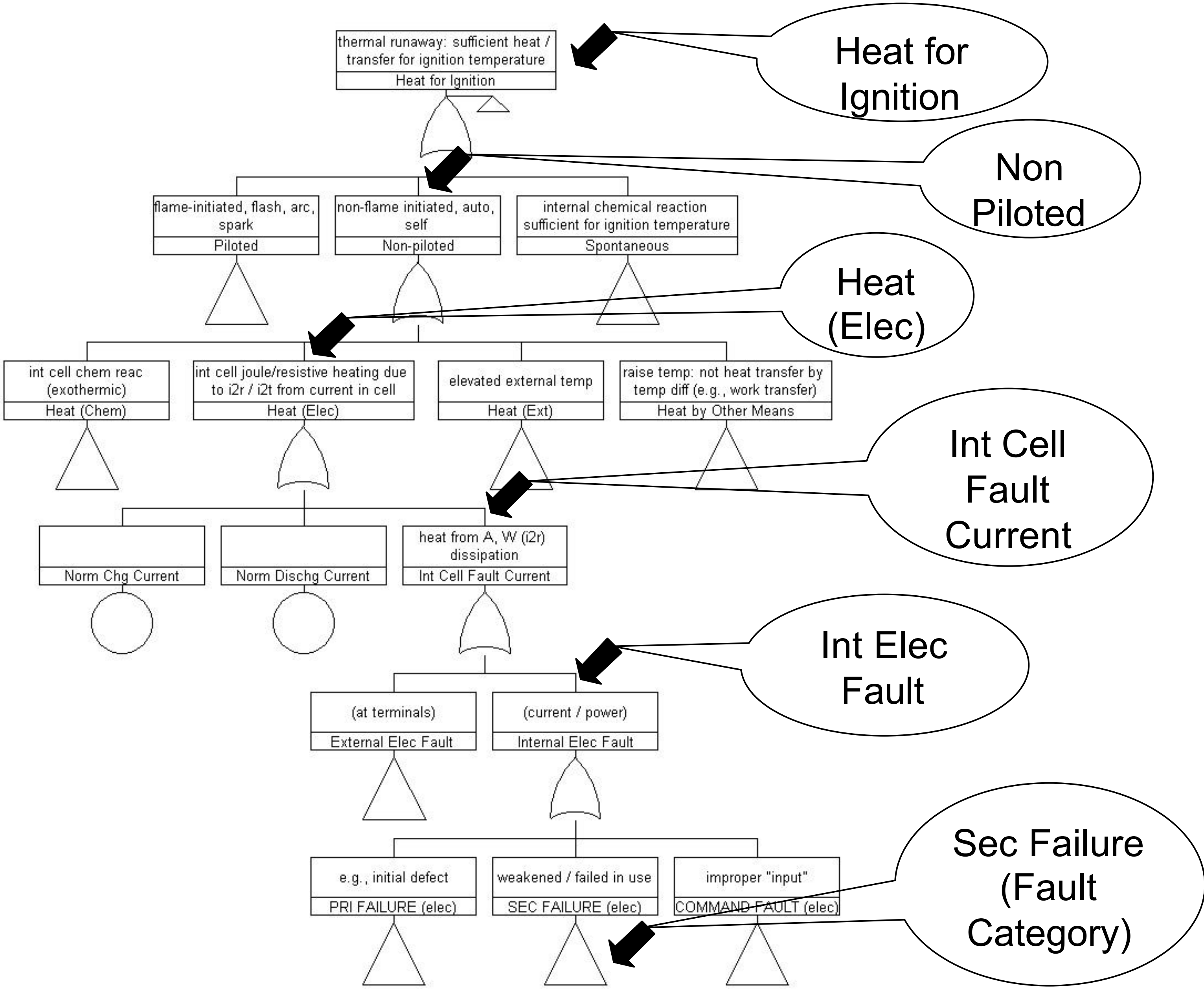
This HBSE Fault Tree model outlines logical relationships among factors that may cause a lithium battery thermal event such as vigorously burning fire or explosive docomposition.

It is based on unwanted generation, conversion and transfer of hazardous energy (thermal) to susceptible parts (unintended fuels).

FTA progresses from general to progressively more specific conditions, drilled down to root causes to identify mechanisms of harm, which may then be prioritized by risk level.

Safeguard strategies, protective mechanisms and the tests that can validate them can then be identified and prioritized.

"Thermal Incident / Event"
"Rapid Disassembly"
"Spontaneous Decomposition"



thermal runaway: sufficient heat / transfer for ignition temperature

Heat for Ignition

flame-initiated, flash, arc, spark

Piloted

non-flame initiated, auto, self

Non-piloted

internal chemical reaction sufficient for ignition temperature

Spontaneous

int cell chem reac (exothermic)

Heat (Chem)

int cell joule/resistive heating due to i2r / i2t from current in cell

Heat (Elec)

elevated external temp

Heat (Ext)

raise temp: not heat transfer by temp diff (e.g., work transfer)

Heat by Other Means

Norm Chg Current

Norm Dischg Current

heat from A, W (i2r) dissipation

Int Cell Fault Current

(at terminals)

External Elec Fault

(current / power)

Internal Elec Fault

e.g., initial defect

PRI FAILURE (elec)

weakened / failed in use

SEC FAILURE (elec)

improper "input"

COMMAND FAULT (elec)

Heat for Ignition

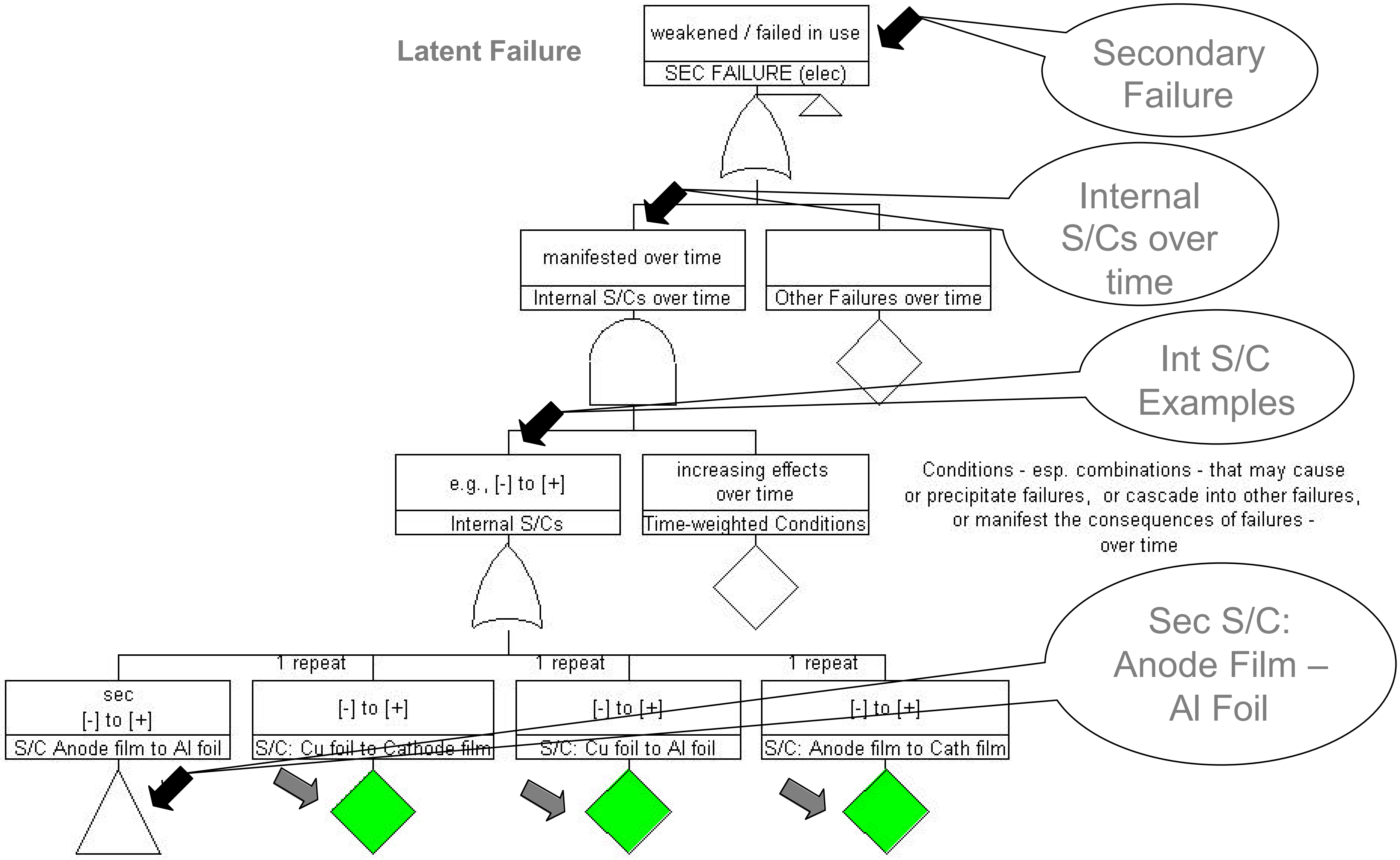
Non Piloted

Heat (Elec)

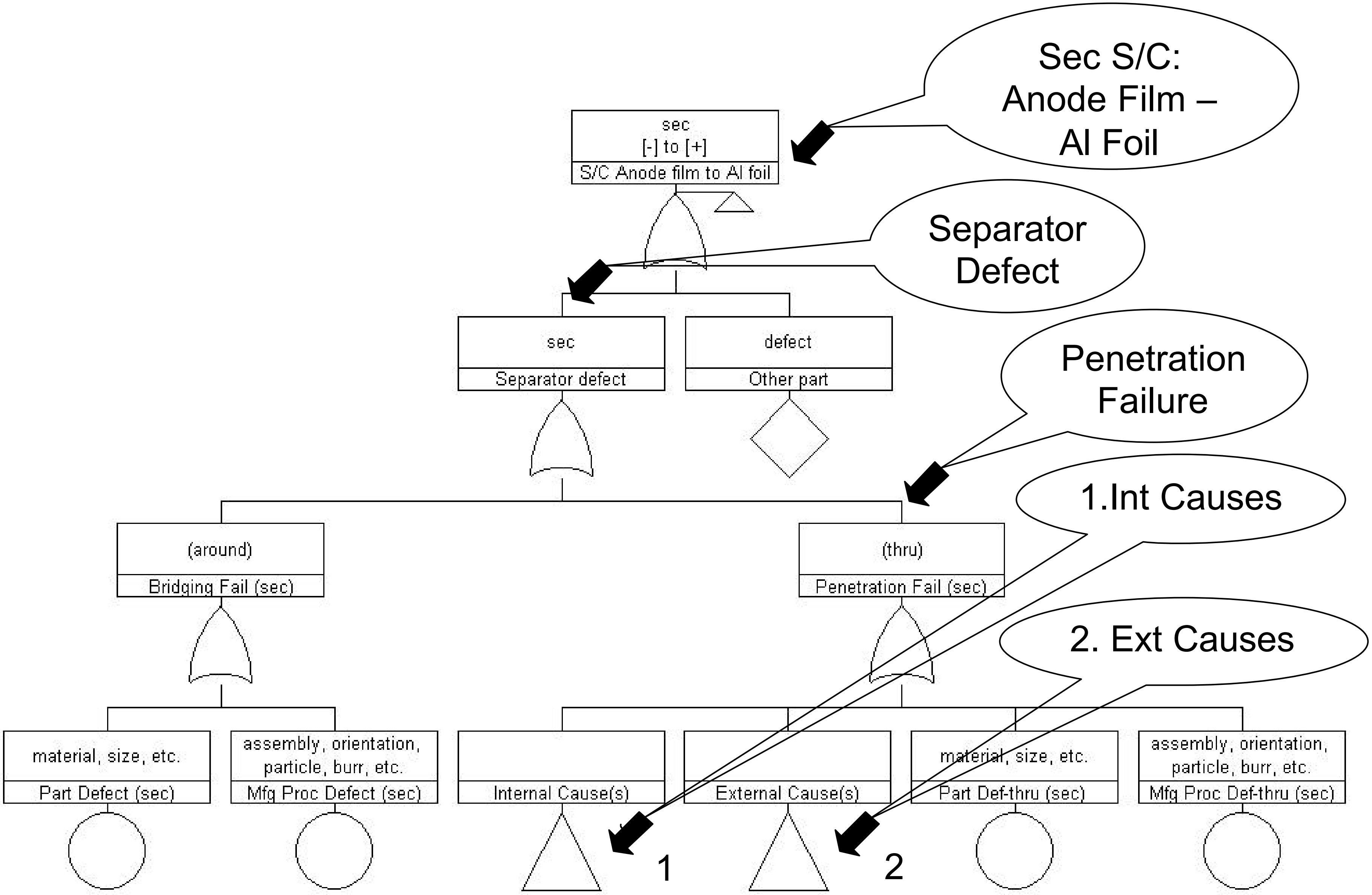
Int Cell Fault Current

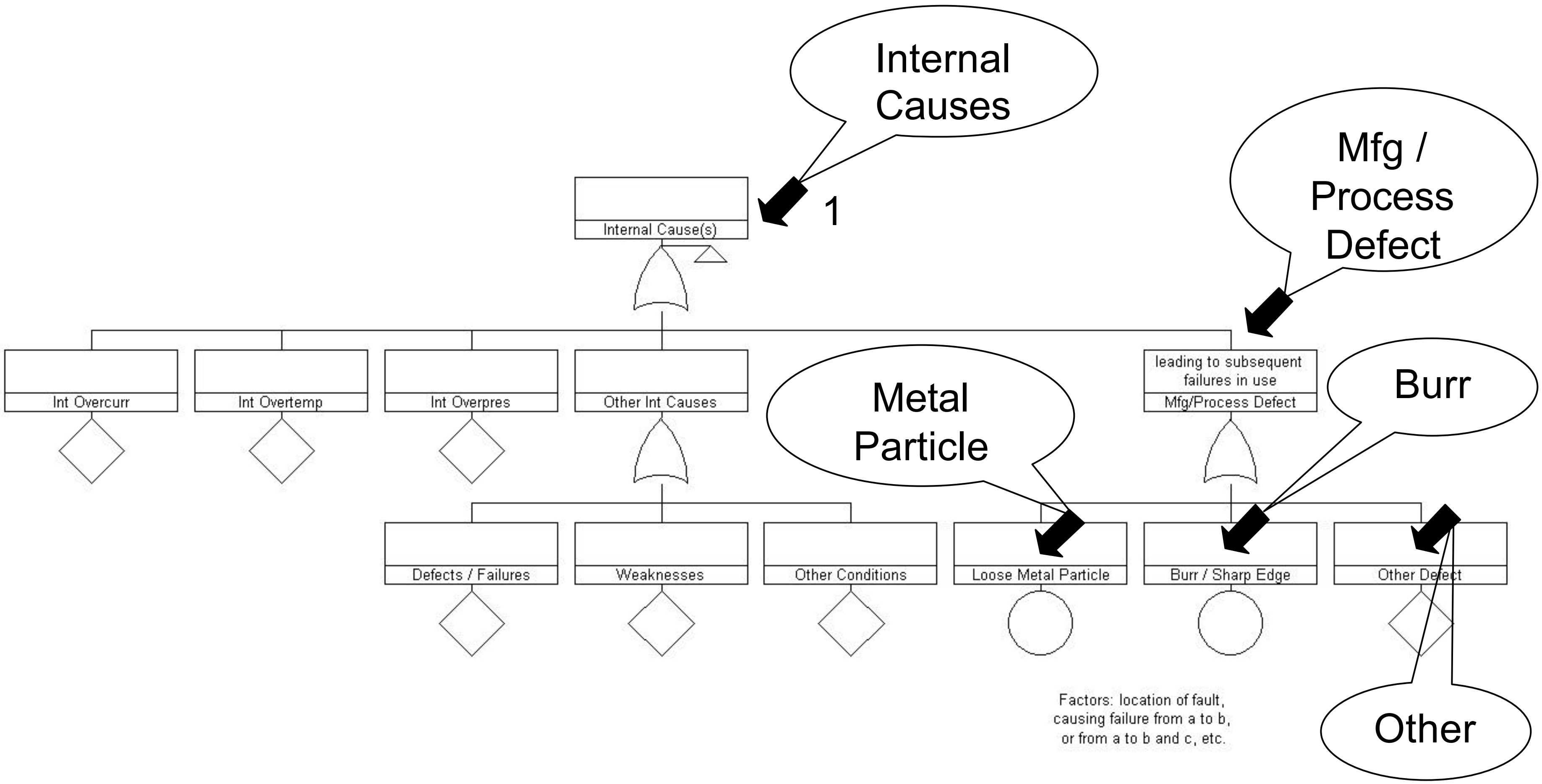
Int Elec Fault

Sec Failure (Fault Category)



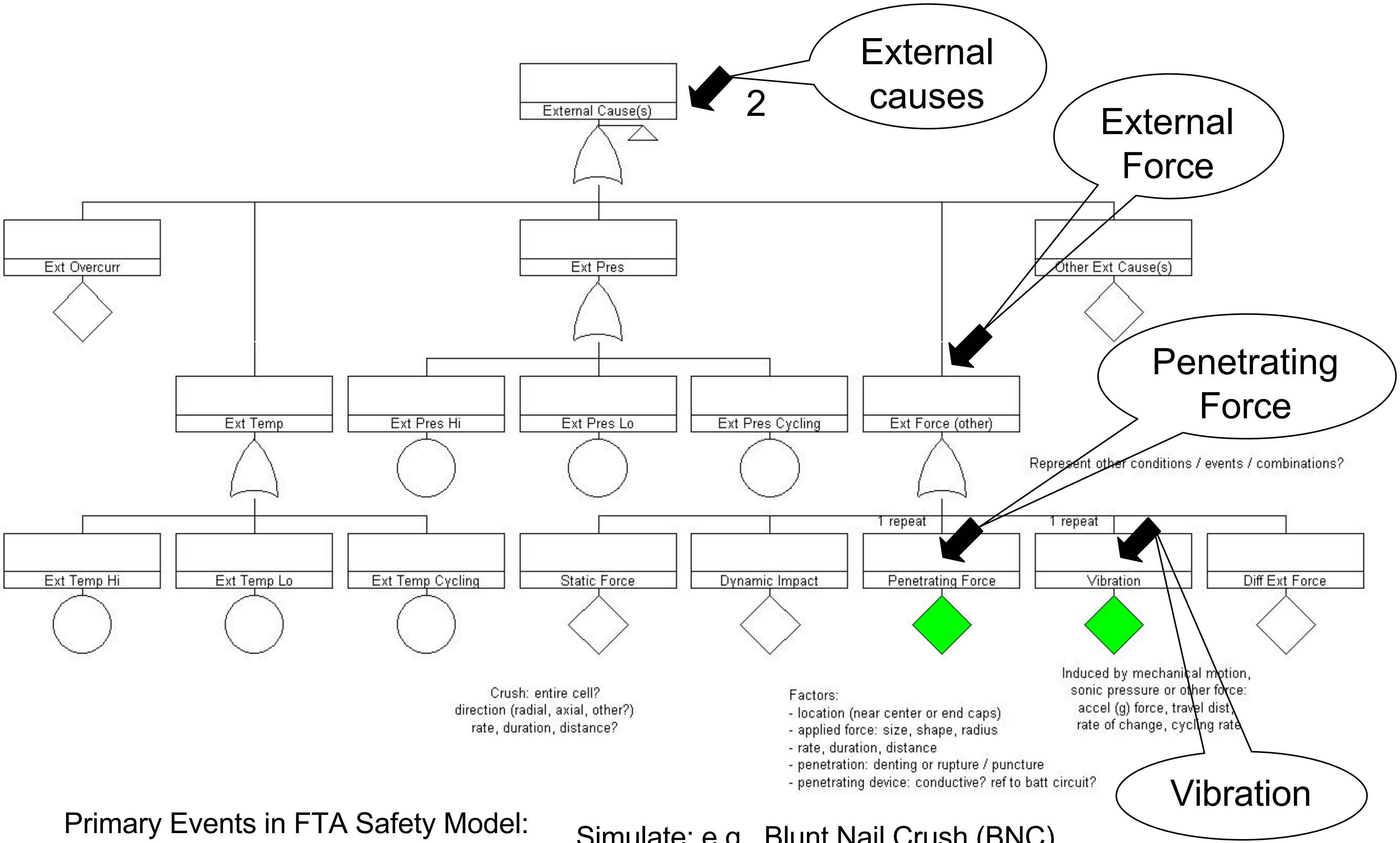
(And one fault can cause, precipitate or cascade into one or more other faults)


Sec S/C:
Anode Film –
Al Foil
sec
[-] to [+]
S/C Anode film to Al foil
Separator
Defect
sec
Separator defect
defect
Other part
Penetration
Failure
1.Int Causes
(around)
Bridging Fail (sec)
(thru)
Penetration Fail (sec)
2. Ext Causes
material, size, etc.
Part Defect (sec)
assembly, orientation, particle, burr, etc.
Mfg Proc Defect (sec)
Internal Cause(s)
External Cause(s)
material, size, etc.
Part Def-thru (sec)
assembly, orientation, particle, burr, etc.
Mfg Proc Def-thru (sec)
1
2



Primary Events in FTA Safety Model:
analyzed as potential failure modes
in FMEA Safety Model

Simulate: e.g., external force
See upcoming presentation: Blunt Nail Crush (BNC)
Internal Short Circuit Lithium-ion Cell Test Method



External causes

2

External Force

Penetrating Force

Vibration

Represent other conditions / events / combinations?

Crush: entire cell?
direction (radial, axial, other?)
rate, duration, distance?

Factors:
- location (near center or end caps)
- applied force: size, shape, radius
- rate, duration, distance
- penetration: denting or rupture / puncture
- penetrating device: conductive? ref to batt circuit?

Induced by mechanical motion,
sonic pressure or other force:
accel (g) force, travel dist,
rate of change, cycling rate

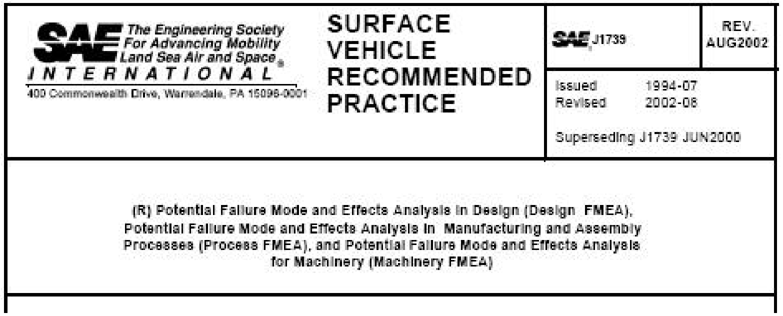
Primary Events in FTA Safety Model:
Analyzed as potential failure modes
in FMEA Safety Model

Simulate: e.g., Blunt Nail Crush (BNC)

the standard in safety

FMEA Safety Model - Overview

Based on standard format / guidelines, e.g., SAE J1739, etc. (adapted for application)



SAE The Engineering Society For Advancing Mobility Land Sea Air and Space INTERNATIONAL
400 Commonwealth Drive, Warrendale, PA 15096-0001

SURFACE VEHICLE RECOMMENDED PRACTICE

SAE J1739

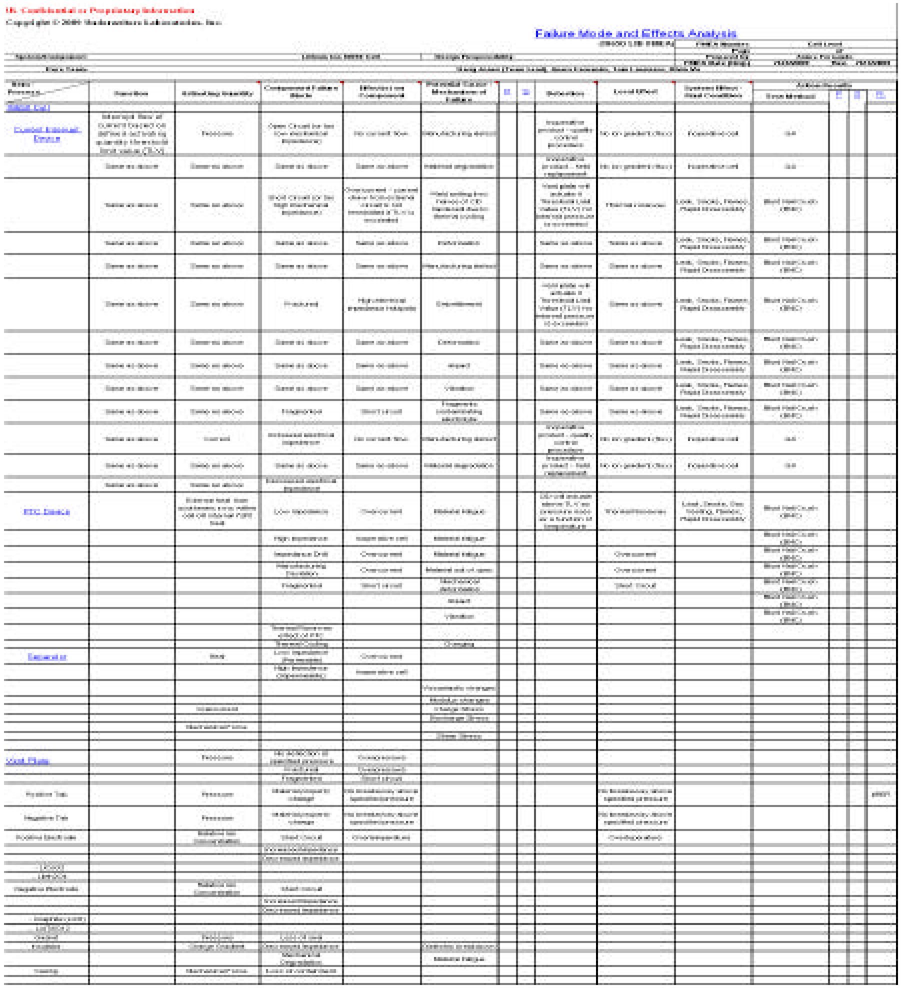
REV. AUG2002

Issued 1994-07
Revised 2002-08

Superseding J1739 JUN2000

(R) Potential Failure Mode and Effects Analysis in Design (Design FMEA), Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA), and Potential Failure Mode and Effects Analysis for Machinery (Machinery FMEA)

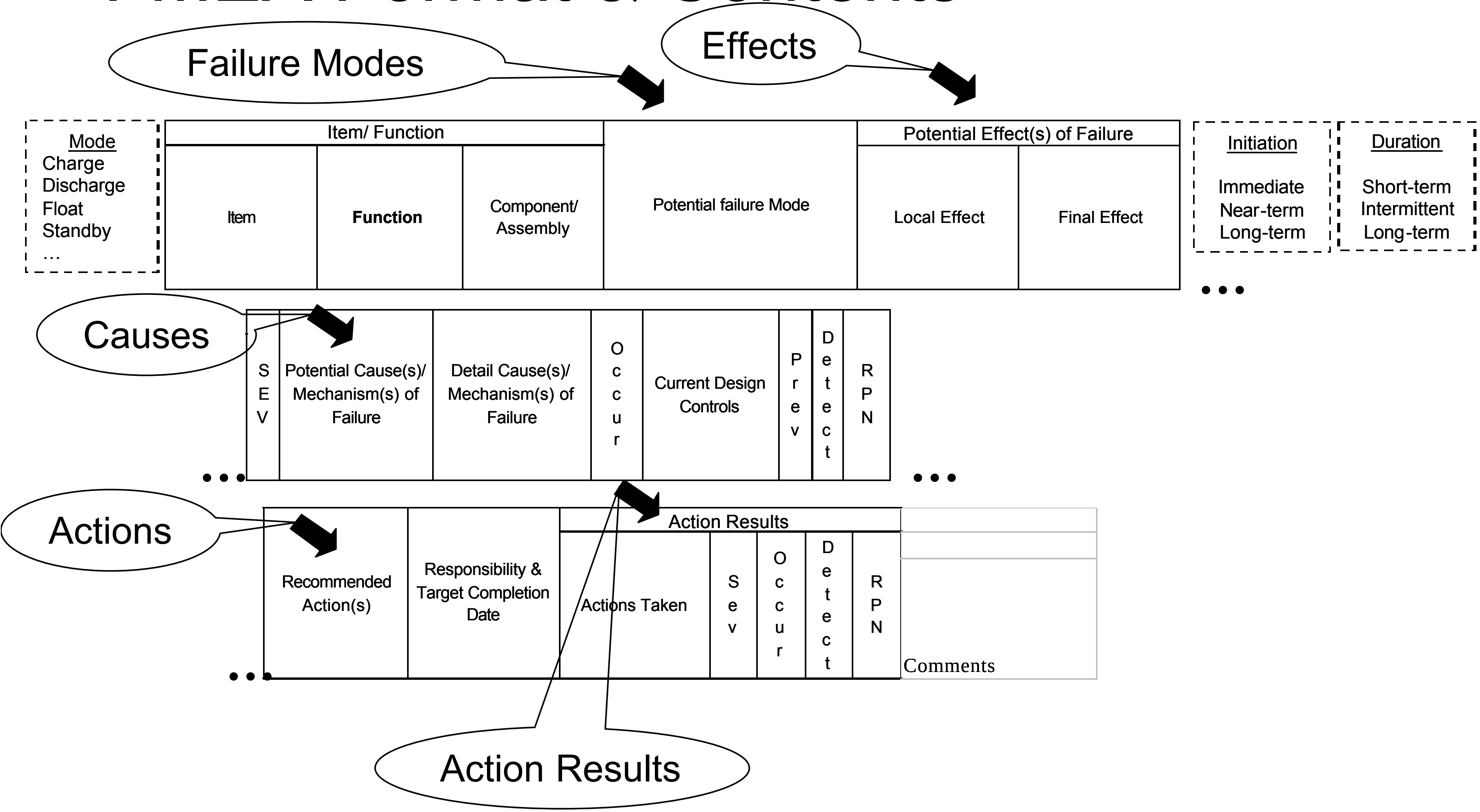
Example FMEA (overall view):



Failure Mode and Effects Analysis

[illegible]

FMEA Format & Contents



Failure Modes

Effects

Mode
Charge Discharge Float Standby …

Item/ Function			Potential failure Mode	Potential Effect(s) of Failure	
Item	Function	Component/ Assembly		Local Effect	Final Effect

Initiation	Duration
Immediate Near-term Long-term	Short-term Intermittent Long-term

• • •

Causes

• • •

SEV	Potential Cause(s)/ Mechanism(s) of Failure	Detail Cause(s)/ Mechanism(s) of Failure	Occur	Current Design Controls	Prev	Detect	RPN

• • •

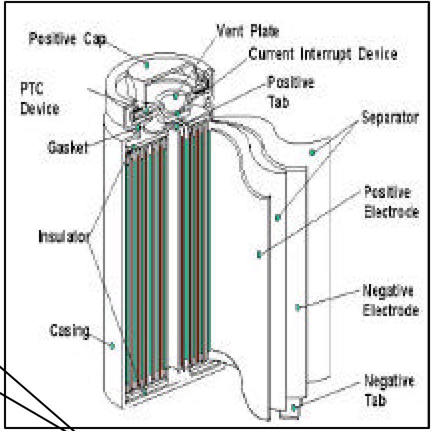
Actions

• • •

Recommended Action(s)	Responsibility & Target Completion Date	Action Results					
		Actions Taken	Sev	Occur	Detect	RPN	Comments

Action Results

FMEA Safety Model: Separator Example



Function

Fail Mode

Effect (Comp)

Cause

Syst Effect

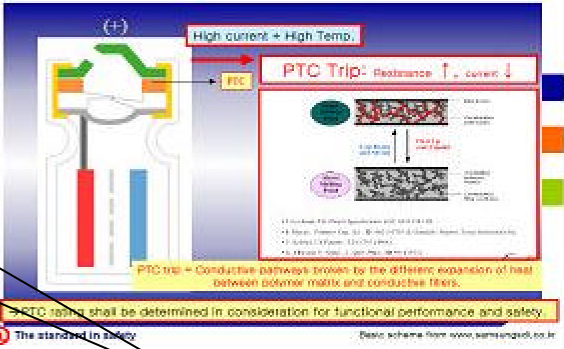
Action / Test

Item / Process	Function	Activating Quantity	Component Failure Mode	Effect(s) on Component	Potential Cause / Mechanism of Failure	P	S	Detection	Local Effect	System Effect - Final Condition	Action Results			
											Test Method	P	S	R.
18650 Cell														
Separator	Anode to Cathode barrier	Heat	Low Impedance (Permeable)	Overcurrent										
	Anode to Cathode barrier		High Impedance (Impermeable)	Inoperative cell										
	Anode to Cathode barrier				Viscoelastic changes									
	Anode to Cathode barrier				Modulus changes									
	Anode to Cathode barrier	Overcurrent			Charge Stress									
	Anode to Cathode barrier				Discharge Stress									
➡	Anode to Cathode barrier	Mechanical Force	Loss of mechanical integrity	Puncture	Metal particle contaminant				Anode to Cathode Short	Leak, Smoke, Flames, Rapid Disassembly (design dependent)	Blunt Nail Crush (BNC)			
	Anode to Cathode barrier				Shear Stress									
	Anode to Cathode barrier													

Validate functionality: simulate via external force, e.g., Blunt Nail Crush (BNC)

See upcoming presentation "Blunt Nail Crush (BNC) Internal Short Circuit Lithium-ion Cell Test Method"

FMEA Safety Model: PTC Example



(+)
PTC
High curent + High Temp.
PTC Trip: Resistance ↑, current ↓
PTC trip = Conductive pathways broken by the different expansion of heat between polymer matrix and conductive fillers.
※PTC rating shall be determined in consideration for functional performance and safety.
The standard in safety
Basic scheme from www.samsungsdi.co.kr

Function

Fail Mode

Effect

Cause

Syst Effect

Action / Test

Item / Process	Function	Activating Quantity	Component Failure Mode	Effect(s) on Component	Potential Cause / Mechanism of Failure	P	S	Detection	Local Effect	System Effect - Final Condition	Action Results			
											Test Method	P	S	R.
18650 Cell														
PTC Device	➡	External heat from exothermic rxns within cell OR internal I^2Rt heat	Low Impedance	Overcurrent	Material fatigue			CID will actuate above TLV as pressure rises as a function of temperature	Thermal Runaway	Leak, Smoke, Gas Venting, Flames, Rapid Disassembly	Blunt Nail Crush (BNC)			
			High Impedance	Inoperative cell	Material fatigue						Blunt Nail Crush (BNC)			
			Impedance Drift	Overcurrent	Material fatigue				Overcurrent		UL 1434			
			Manufacturing Deviation	Overcurrent	Material out of spec				Overcurrent		Blunt Nail Crush (BNC)			
			Fragmented	Short circuit	Mechanical deformation				Short Circuit		Blunt Nail Crush (BNC)			
					Impact						Blunt Nail Crush (BNC)			
					Vibration						Blunt Nail Crush (BNC)			
			Thermal Runaway effect of PTC											
			Thermal Cycling		Charging									

Validate functionality: Simulate: e.g., Blunt Nail Crush (BNC)

E.g., PTC relied on as external short circuit protection, but in functioning, heat dissipated should not spread and result in other failures that may lead to hazards and harm (internal shorts) (Safeguards should not introduce or increase other hazards)

FTA / FMEA Characteristics

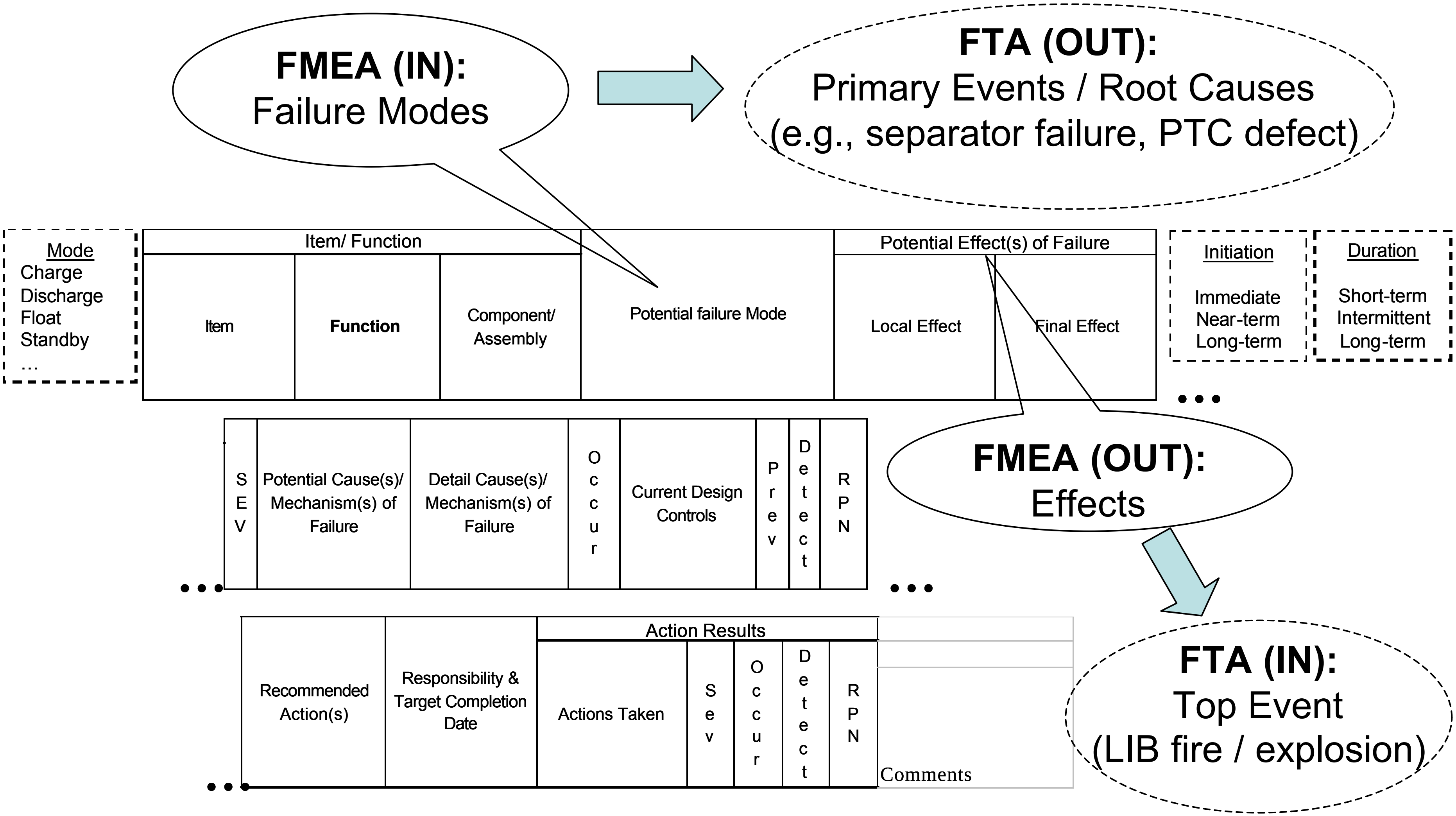
FTA	***FMEA***
Deductive / Top-down	Inductive / Bottom-up
Graphical / Diagrammatic	Tabular
Parallel	Serial
General → Specific	Specific → General
IN: System Fault (General)	IN: Failure Modes (Specific)
OUT: Root Causes (Specific)	OUT: System Effects (General)
PROCESS: Contributing, precipitating, cascading conditions / events / relationships. Preventive / mitigating protection means	PROCESS: Items, functions, operating modes / conditions, causes, protective means and effects

Integrated FTA / FMEA Safety Model

- Systematic, Structured, Disciplined
- Qualitative / Quantitative / Comparative
- Guided / Documented Analytical Process: IN → OUT
- Complementary / Supplementary / Synergistic

- Safety, not performance or other functional aspects
- Model – necessarily broader than specific analysis
- Purpose / Intent – One size fits many

FMEA Integration with FTA



FMEA (IN):
Failure Modes

FTA (OUT):
Primary Events / Root Causes
(e.g., separator failure, PTC defect)

Mode
Charge
Discharge
Float
Standby
…

Item/ Function			Potential failure Mode	Potential Effect(s) of Failure	
Item	**Function**	Component/ Assembly		Local Effect	Final Effect

Initiation
Immediate
Near-term
Long-term

Duration
Short-term
Intermittent
Long-term

• • •

FMEA (OUT):
Effects

• • •

SEV	Potential Cause(s)/ Mechanism(s) of Failure	Detail Cause(s)/ Mechanism(s) of Failure	Occur	Current Design Controls	Prev	Detect	RPN

• • •

FTA (IN):
Top Event
(LIB fire / explosion)

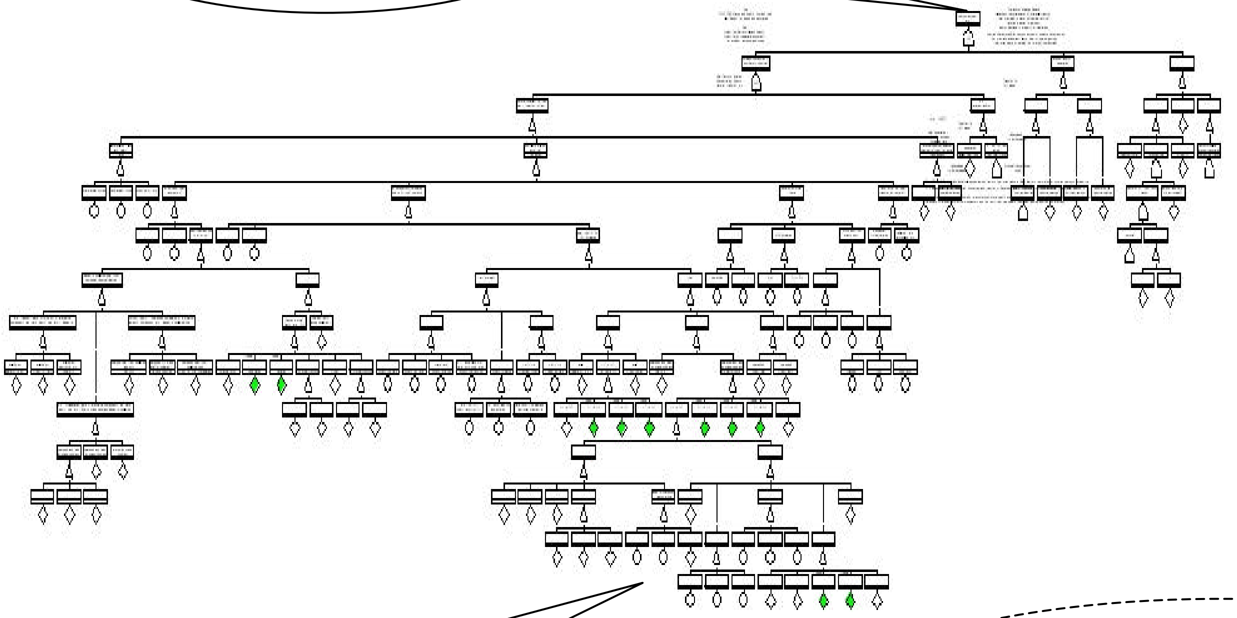
• • •

Recommended Action(s)	Responsibility & Target Completion Date	Action Results					
		Actions Taken	Sev	Occur	Detect	RPN	Comments

FTA Integration with FMEA

FTA (IN):
Top Event Fault

FMEA (OUT):
Effects (LIB fire / explosion)



FTA (OUT):
Root Causes

FMEA (IN):
Failure Modes
e.g., separator failure, PTC defect

Conclusions

- Safety Analyses: systematic & robust
- Integrated FTA / FMEA Safety Models:
  - Methodically analyze and reduce risk
  - Complementary: more effective predictive modeling
  - Scaleable: simple to complex
  - Identify / prioritize specific means of protection
  - Prevent occurrence and/or mitigate severity

Mutual Benefits:

- Demonstrate Safety Improvements
- Tie Together Conducted Research
- Identify / Prioritize Future Research

Next Steps

- Techniques, tools, team integration
  - Further develop: breadth/depth, internal/external
- Scope of analysis and requirements
  - Refine, adapt, expand as needed
- Test Methodologies – (pre)conditions, methods, measurements, criteria
  - Further develop / refine

Thank You

Comments / Questions?